UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

23117 7590 03/20/2009

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
WITZENBURG, BRUCE A	
ART UNIT	PAPER NUMBER
2166	

DATE MAILED: 03/20/2009

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/588,657	08/07/2006	Glen J. Slade	34-134	9244

TITLE OF INVENTION: DATA STORAGE

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$755	$300	$0	$1055	06/22/2009

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

23117 7590 03/20/2009

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (57I) 273-2885, on the date indicated below.

(Depositor's name)

(Signature)

(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/588,657	08/07/2006	Glen J. Slade	34-I34	9244

TITLE OF INVENTION: DATA STORAGE

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$755	$300	$0	$1055	06/22/2009

EXAMINER	ART UNIT	CLASS-SUBCLASS
WITZENBURG, BRUCE A	2I66	707-I02000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

□ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

□ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(I) the names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

I ____________________

2 ____________________

3 ____________________

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.II. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : □ Individual □ Corporation or other private group entity □ Government

4a. The following fee(s) are submitted:

□ Issue Fee

□ Publication Fee (No small entity discount permitted)

□ Advance Order - # of Copies ____________________

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

□ A check is enclosed.

□ Payment by credit card. Form PTO-2038 is attached.

□ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number ____________ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

□ a. Applicant claims SMALL ENTITY status. See 37 CFR I.27.

□ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature ______________________________ Date ______________________________

Typed or printed name ______________________________ Registration No. ______________________________

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/588,657	08/07/2006	Glen J. Slade	34-134	9244

23117 7590 03/20/2009

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
WITZENBURG, BRUCE A	
ART UNIT	PAPER NUMBER
2166	

DATE MAILED: 03/20/2009

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)

(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 106 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 106 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Notice of Allowability	**Application No.** 10/588,657	**Applicant(s)** SLADE, GLEN J.	
	Examiner BRUCE A. WITZENBURG	**Art Unit** 2166	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *Remarks filed 3/09/2009*.

2. ☒ The allowed claim(s) is/are *64-136*.

3. □ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a) ☒ All b) □ Some* c) □ None of the:

   1. ☒ Certified copies of the priority documents have been received.
   2. □ Certified copies of the priority documents have been received in Application No. _____ .
   3. □ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. □ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. □ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.

   (a) □ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached

   1) □ hereto or 2) □ to Paper No./Mail Date _____.

   (b) □ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. □ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. □ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. □ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. □ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. □ Notice of Informal Patent Application
6. □ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. □ Other _____.

/Etienne P LeRoux/ Primary Examiner, Art Unit 2161	/Bruce A Witzenburg/ Examiner, Art Unit 2166

DETAILED ACTION

1. Claims 64-136 are pending in the instant application.

EXAMINER'S AMENDMENT

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

3. The application has been amended as follows:

Claims 1-63 (Cancelled)

64. (Currently amended) A method of storing a data set on a storage device having one or more portions of random data comprising:

determining using a process dependent upon a user input passphrase, a first storage writing process starting location at a first offset within ~~a~~ one of the portions of random data for initiating a first storage writing process for storing a file index;

determining a second storage writing process starting location at a second offset within ~~a~~ one of the portions of random data for initiating a second storage writing process for storing the data set, said second offset determined using a process that is independent of ~~a~~ the process used to generate said first offset;

encrypting the data set;

writing the encrypted data set using the second storage writing process beginning at the second storage writing process starting location in ~~a~~ one of the portions of random data;

creating ~~a~~ the file index including an entry in the file index in respect of the data set, the entry comprising an indication of the second storage writing process starting location;

encrypting the file index; and

writing the encrypted file index using the first storage writing process beginning at the first storage writing process starting location in one of the ~~file~~ portions of random data.

.

65. (Currently amended) A method of operating a computer to store a data set on a storage device, comprising:

determining a first location at a first offset within the storage device for initiating a first storage writing process for storing a file index;

determining a second storage writing process starting location at a second offset within the storage device for storing the data set, said second offset determined using a process that is independent of a process used to generate said first offset;

encrypting the data set;

writing the encrypted data set using ~~the~~ a second storage writing process beginning at the second storage writing process starting location in a portion of random data;

creating ~~a~~ the file index including an entry in the file index in respect of the data set, the entry comprising an indication of the second storage writing process starting location;

encrypting the file index; and

writing the encrypted file index using the first storage writing process beginning at the first storage writing process starting location.

66. (Previously presented) The method according to claim 64 in which the determining the first storage writing process starting location for creating the file index comprises adding a predetermined offset to the first storage writing process starting location as a beginning of the file index.

67. (Previously presented) The method according to claim 64 wherein the encrypted file index is stored only within the portions of random data on the device.

68. (Currently amended) The method according to claim 64 in which ~~an~~ the encrypted file index is stored within one or more of the portions of random data by writing over random data portions within the storage device with the encrypted file index data.

69. (Previously presented) The method according to claim 64 wherein the encrypted data set is stored only within the portions of random data.

70. (Currently amended) The method according to claim 64 in which ~~an~~ the encrypted data set is stored within one or more of the portions of random data by writing over random data portions within the storage device with the encrypted data set.

71. (Previously presented) The method according to claim 64 which further comprises a using the user input passphrase for generating a key for encrypting the file index.

72. (Previously presented) The method according to claim 64 in which the passphrase is used for generating a key for encrypting the data set.

73. (Previously presented) The method according to claim 64 in which the passphrase is used in selecting the second storage writing process starting location.

74. (Currently amended) The method according to claim 64 in which at least one of the first location within one of the ~~file~~ portions of random data, the second location within one of the ~~file~~ portions of random data, a key for the file index and a key for the data set is determined by using at least one hash function to operate on the user input passphrase.

75. (Currently amended) The method according to claim 64 in which the passphrase is operated on once to produce an output which is used for determining at least two of the first location within one of the ~~file~~ portions of random data, the second location within one of the ~~file~~ portions of random data, a key for the file index and a key for the data set.

76. (Currently amended) The method according to claim 64 in which the passphrase is operated on a plurality of times, each operation generating an output for use in

determining at least one of the first location within one of the ~~file~~ portions of random data, the second location within one of the ~~file~~ portions of random data, a key for the file index and a key for the data set.

77. (Previously presented) The method according to claim 64 in which a common key is used for encrypting the data set and for encrypting the file index.

78. (Previously presented) The method according to claim 64 which comprises a step of storing further sets of data using said passphrase.

79. (Previously presented) The method according to claim 78 which is such that a respective location for each data set is selected, each data set is encrypted and stored at the respective location, and respective entries are added to the file index.

80. (Currently amended) The method according to claim 64, comprising a step of storing further file indexes within one of the ~~file~~ portions of random data, each of which ~~indexes~~ is associated with a respective passphrase and each of which ~~indexes~~ is encrypted and is stored at a location selected in dependence on the respective passphrase.

81. (Previously presented) The method according to claim 80 in which respective encryption keys are generated from the respective passphrases and these respective keys are used for encrypting data sets which are associated with each file index.

82. (Currently amended) The method according to claim 80 comprising a step of selecting the passphrase for, and hence location for, an additional file index with knowledge of the respective passphrases corresponding to file indexes already stored in one of the ~~file~~ portions of random data such that collisions may be avoided.

83. (Currently amended) The method according to claim 80, in which, ~~where~~ there are a plurality of file indexes stored in one of the ~~file~~ portions of random data, the method comprises a step of selecting a location for an additional data set with knowledge of the respective passphrases corresponding to file indexes already stored in one of the ~~file~~ portions of random data such that collisions may be avoided.

84. (Currently amended) The method according to claim 80 comprising a step of storing additional data sets using an additional passphrase whilst in ignorance of at least one other existing passphrase.

85. (Currently amended) The method according to claim 80 comprising a step of storing data sets in a predetermined relationship to a respective file index to help prevent collisions, for example the data sets may be stored adjacent to ~~a~~ the respective file index, the data sets may be stored substantially contiguously to ~~a~~ the respective file index, and the data sets may be stored at locations close to but after ~~a~~ the respective

file index.

86. (Currently amended) The method according to claim 64 comprising a step of storing data on ~~a~~ the storage device carrying a plurality of files of random data.

87. (Previously presented) The method according to claim 64 in which the file index comprises a message authentication code.

88. (Previously presented) The method according to claim 87 in which the file index comprises a message authentication code of all associated data sets so as to facilitate detection of tampering.

89, (Currently amended) The method according to claim 87 in which the file index comprises a message authentication code of one of the ~~file~~ portions of random data in its entirety for use in detecting other usage of one of the ~~file~~ portions of random data.

90. (Previously presented) The method according to claim 64 comprising a step of pre processing the data set prior to encryption.

91. (Currently amended) The method according to claim 64 comprising a step of presenting a user with an indication of a location within one of the ~~file~~ portions of random data that will be selected for the file index when using a predetermined

passphrase,

92. (Currently amended) The method according to claim 91 comprising a step of accepting user entered trial passphrases and providing a user with an indication of a location within one of the ~~file~~ portions of random data that will be selected for the file index for each trial passphrase.

93. (Currently amended) The method according to claim 91 comprising a further step of providing to ~~a~~ the user an indication of the regions of one of the ~~file~~ portions of random data that are already occupied by file indexes having passphrases that have been supplied by ~~a~~ the user.

94. (Currently amended) The method according to claim 64 comprising a step of receiving an indication from a user of a location within one of the ~~file~~ portions of random data which ~~a~~ the user desires to use for ~~a~~ the file index.

95. (Currently amended) The method according to claim 94 further comprising ~~the~~ a step of suggesting possible passphrases to ~~a~~ the user in response to ~~a~~ the user indicating a location within one of the ~~file~~ portions of random data which ~~a~~ the user desires to use for ~~a~~ the file index,

96. (Previously presented) The method according to claim 94 comprising steps of receiving a user input passphrase and suggesting a modified passphrase.

97. (Previously presented) The method according to claim 96 in which the modification of the passphrase is selected so as to at least one of: move a location at which an associated index would be stored towards a desired location indicated by a user and strengthen the passphrase,

98. (Currently amended) The method according to claim 64 comprising a step of deleting ~~a~~ the data set stored on ~~a~~ the storage device.

99. (Previously presented) The method according to claim 98 comprising a step of removing a respective entry from the file index.

100. (Currently amended) The method according to claim 99 in which the step of deleting ~~a~~ the data set comprises a step of overwriting the data set with random data as well as removing the entry from the file index.

101. (Currently amended) The method according to claim 98 comprising a step of reorganizing data stored in association with ~~a~~ the file index when at least one data set referenced in that file index is deleted.

102. (Currently amended) The method according to claim 100 in which the step of overwriting the data set comprises a step of using at least one random data and encrypted data stored in one of the ~~file~~ portions of random data for generating pseudo-random data for overwriting deleted files.

103. (Currently amended) The method according to claim 102 in which the method comprises a step of using random numbers from one of the ~~file~~ portions of random data that would be overwritten when adding a further data set to replace any pseudo-random values previously used elsewhere within one of the ~~file~~ portions of random data.

104. (Previously presented) A computer storage device for steganographically concealing stored information, said device configured with at least one storage area having one or more portions of random data containing a file index and a predetermined data set, and software carrying out steps wherein the file index is encrypted and is stored at a first location determined by an algorithmic process dependent upon a user passphrase, and the data set is encrypted and is stored at a second location determined using a process that is unconstrained by the process used to determine the first location, and the file index comprises an information indicative of the second location.

105. (Previously presented) The storage device according to claim 104 further including application software stored thereon for execution by a computer to enable

steganographic storage extraction of data sets in the one or more portions of random data.

106. (Previously presented) The storage device according to claim 104 in which the passphrase is used to generate a key for at least one of encrypting the file index and encrypting the data set.

107. (Currently amended) The storage device according to claim 104 further comprising a software application stored by the storage device, the software comprising instructions that when loaded and executed by a computer cause the computer to perform at least one of the following operations:

accepting a plurality of user input passphrases and generating corresponding encryption/decryption keys;

determining respective storage writing process starting locations for storage of a plurality of ~~storage of~~ file indexes;

encrypting ~~a~~ the plurality of file indexes;

encrypting data sets;

storing ~~a~~ the plurality of file indexes;

determining respective storage writing process starting locations for storing a plurality of data sets;

storing ~~a~~ the plurality of data sets;

accepting one or more user input passphrases and using said one or more user input passphrases for locating and decrypting the respective file indexes;

locating one or more encrypted data sets stored within the storage device: decrypting the one or more encrypted data sets stored within the storage device; and

outputting the one or more decrypted data sets stored within the storage device as an encrypted data set.

108, (Previously presented) The storage device according to claim 104 further including a conventional file allocation table stored thereon.

109, (Previously presented) The storage device according to claim 104 wherein at least a portion of the device comprises a Read Only Memory (ROM).

110. (Currently amended) The storage device according to claim 108 further comma Read Only Memory (ROM) portion wherein is stored the file allocation table, ~~the~~ software and an operating system header file.

111. (Previously presented) The storage device according to claim 104 wherein the device is operable as a removable storage device.

112. (Previously presented) The storage device according to claim 104 wherein the device is assigned a particular identifying serial number.

113. (Currently amended) The storage device according to claim 104 further including a unique hard coded identifier data stored in memory contained therein said identifier data for use by a computer for at least one of:

a) an encryption process used for encrypting at least one of the file index and the data set; and

b) a decryption process used for decrypting at least one of the file index and the data set.

114. (Previously presented) The storage device according to claim 104 wherein the storage device has the appearance of a conventional portable memory storage device.

115, (Currently amended) A computer arranged under the control of software, said computer executing software instructions for steggnographically storing a data set on a storage device within one or more portions of random data contained on said storage device, said computer comprising:

programmable logic circuitry configured to determine a first location within the storage device for initiating a first storage writing process for storing a file index;

selecting programmable logic circuitry configured to determine a second storage writing process starting location at a second offset within the storage device for storing the data set where said storage writing process starting location is determined independently from the process used to select the first location;

programmable logic circuitry configured to encrypt the data set;

programmable logic circuitry configured to write the encrypted data set using ~~the~~ a the second storage writing process beginning at the second storage writing process starting location in a portion of random data;

programmable logic circuitry configured to create a file index including an entry in the file index in respect of the data set, the entry comprising an indication of the second storage writing process starting location;

programmable logic circuitry configured to encrypt the file index; and programmable logic circuitry configured to write the encrypted file index using the first storage writing process beginning at the first storage writing process starting location in the ~~file~~ portion of random data.

116. (Previously presented) The computer according to claim 115 further comprising programmed logic circuitry configured by said software to provide a user with an indication of a location within a portion of random data that will be used for storing the file index corresponding to a particular, passphrase input by a user.

117. (Currently amended) The computer according to claim 115 which is arranged under the control of software to accept user entered trial passphrases and provide a user with an indication of a location within the ~~file~~ portion of random data that will be selected for storing the file index for each trial passphrase.

118. (Currently amended) The computer according to claim 115 which is arranged under the control of software to provide a user an indication of regions of the ~~file~~ portion of random data that are already occupied by file indexes having passphrases that have been supplied by a user.

119. (Currently amended) The computer according to claim 115 which is arranged under the control of software to suggest possible passphrases to a user in response to a user indicating a location within the ~~file~~ portion of random data which a user desires to use for storing ~~a~~ the file index.

120. (Previously presented) The computer according to claim 116 which is arranged under the control of software to present a user interface for displaying the indication~~s~~.

121, (Currently amended) The computer according to claim 120 in which the user interface is arranged so that a user can use a pointing device to indicate a location within the ~~file~~ portion of random data which a user desires to use for storing ~~a~~ the file index.

122. (Currently amended) A method of extracting a data set steganographically stored on a storage device having one or more portions random data containing a file index and a predetermined data set, wherein the file index is encrypted and is stored at a first

location determined by an algorithmic process dependent upon a user input passphrase, and the data set is encrypted and is stored at a second location determined using a process that is unconstrained by the process used to determine the first location, and the file index comprises information indicative of the second location, comprising:

using a user input passphrase to determine a location for ~~a~~the file index based upon the user input passphrase;

decrypting the file index;

identifying a location of ~~a~~the data set from the decrypted file index; and decrypting the data set stored at the identified location.

123. (Currently amended) A computer arranged under the control of software to extract data using ~~T~~the method according to claim 122.

124. (Currently amended) A method of storing a data set on a storage device comprising:

determining a first location within the storage device for initiating a first storage writing process for storing a file index;

determining a second storage writing process starting location at a second offset within the storage device for storing the data set,. said second offset

determined using a process that is independent of a process used to generate said first ~~offset~~ location;

encrypting the data set;

writing the encrypted data set using ~~the~~ a second storage writing process beginning at the second storage writing process starting location in a portion of random data;

creating a file index including an entry in the file index in respect of the data set, the entry comprising an indication of the second storage writing process starting location;

encrypting the file index; and

writing the encrypted file index using the first storage writing process beginning at the first storage writing process starting location, ~~wherein~~ the method further comprising~~es~~, prior to a user finalizing ~~the~~ a user input passphrase, accepting input of at least one user input trial passphrase and providing a user with an indication of a location within the portion of random data that will be determined for creating ~~a~~ the file index associated with the at least one user input trial passphrase.

125. (Currently amended) A computer readable data storage medium, said storage medium storing a computer program comprising code portions which when executed a computer cause the computer to perform steps of:

determining a first location within the storage ~~device~~ medium for initiating a first storage writing process for storing a file index;

determining a second storage writing process starting location at a second offset within the storage ~~device~~ medium for storing ~~the~~ a data set said second offset determined using a process that is independent of a process used to determine said first location ~~offset~~; encrypting the data set;

writing the encrypted data set using ~~the~~ a second storage writing process beginning at the second storage writing process starting location in a portion of random data;

creating ~~a~~ the file index including an entry in the file index in respect of the data set, the entry comprising an indication of the second storage writing process starting location;

encrypting the file index; and

writing the encrypted file index using the first storage writing process beginning at the first storage writing process starting location in the portion ~~file~~ of random data.

126. (Currently amended) A method of storing a data set on a storage device having a data storage area that is initialized with one or more portions of ~~a data storage area that are initialized with~~ random data comprising the steps of

determining a first writing process starting location within a data storage portion initialized with random data for creating a file index;

determining a second writing process starting location within a data storage portion initialized with random data for storing the data set, said second writing process starting location determined using a process that is unconstrained by a process used to determine said first writing process starting location;

encrypting the data set;

storing the encrypted data set beginning at the second writing process starting location, using only data storage portions initialized with random data;

making an entry in the file index indicative of which portions of the data storage device initialized with random data are to be used to store the data set, wherein an indication of the second writing process starting location is determinable from the file index; encrypting the file index; and storing the encrypted file index at the first ~~selected~~ determined location in the data storage area initialized with random data.

127. (Currently amended) The method according to claim 126 wherein the step of ensuring that an indication of the second ~~selected~~ determined location is determinable from the file index comprises the step of

making an entry in the file index in respect of the data set, the entry comprising an indication of the second ~~selected~~ determined location.

128. (Currently amended) The method according to claim 126 wherein the step of ~~selecting~~ determining a first location within the data storage area initialized with random data for storing ~~a~~ the file index, comprises

the step of ~~selecting~~ determining the first location from a plurality of predetermined possible locations within the data storage area initialized with random data, in dependence on one of: an input received from a user; and a selection process which is independent of user input.

129. (Currently amended) The method according to claim 126 wherein the step of ~~selecting~~ determining a first location within the data storage area initialized with random data for storing a file, comprises steps of selecting the first location in dependence on a

user input passphrase and associating the file index with the user input passphrase.

130. (Previously presented) The method according to claim 129 wherein said data set is stored under protection of said user input passphrase and the method comprising a further step of storing a second data set on the storage device under protection of a second user input passphrase, the step of storing the second data set on the storage device comprising steps of:

selecting, in dependence on the second user input passphrase, a third location within the data storage area initialized with random data for storing a second file index;

selecting a fourth location within the data storage area initialized with random data for storing the second data set;

encrypting the second data set;

storing the encrypted second data set at the fourth selected location in the data storage area initialized with random data;

ensuring that an indication of the fourth selected location is determinable from the second file index;

encrypting the second file index; and storing the encrypted second file index at the third selected location in the data storage area initialized with random data, and comprising, before the step of encrypting the second file index, a further step of recording in the second file index an indication of which parts of the data storage area initialized with random data will be used to store said second data set.

131. (Previously presented) The method according to claim 126 wherein the data storage area initialized with random data is reserved for use in storing data.

132. (Previously presented) The method according to claim 126 wherein the data storage area initialized with random data comprises a file of random data which is managed by a conventional file system on a computer.

133. (Currently amended) A removable storage device comprising a data storage area initialized with random data, wherein a file index and a data set are stored in the data storage area initialized with random data, and software carrying out steps wherein the file index is encrypted and stored at a first location within the data storage area initialized with random data, the data set is encrypted and stored at a second location within the data storage area initialized with random data where said second location is determined independently from the process used to determine the first location, the file index comprises an entry in respect of the data set, the entry comprising an indication of the second location within the data storage area initialized with random data, and the file index comprises an indication of which parts of the data storage area initialized with random data are in use to store said data set.

134. (Currently amended) A removable storage device carrying software and comprising a data storage area initialized with random data, the software comprising code portions which when loaded and run on a computer cause the computer to

execute a method of storing a data set on the storage device, the method comprising the steps of:

selecting a first location within the data storage area initialized with random data for storing a file index;

selecting a second location within the data storage area initialized with random data for storing the data set where said second location is determined independently from the process used to select the first location;

encrypting the data set;

storing the encrypted data set at the second selected location in the data storage area initialized with random data;

ensuring that an indication of the second selected location is determinable from the file index;

encrypting the file index; and

storing the encrypted file index at the first selected location in the data storage area initialized with random data, and comprising, before the step of encrypting the file index, a further step of recording in the file index an indication of which parts of the data storage area initialized with random data will be used to store said data set.

135. (Original) A method of storing a data set on a storage device having one or more portions of random data, comprising:

determining a first storage writing process starting location at a first offset within a portion of random data for initiating a first storage writing process for storing a data set;

determining a second storage writing process starting location at a second offset within a portion of random data for initiating a second storage writing process that creates a file index,

said second offset determined independently from a process used to generate the first offset;

encrypting the data set;

writing the encrypted data set using said first storage writing process beginning at said first storage writing process starting location;

creating a file index having an entry in respect of the data set, the entry comprising at least an indication of the first storage writing process starting location;

encrypting the file index; and

writing the encrypted file index using said second storage writing process beginning at said second storage writing process starting location.

136. (Original) The method of claim 135 wherein said second offset is determined using an algorithm that is dependent upon an input passphrase.

Allowable Subject Matter

4. Claims 64-136 are allowed.

The following is an examiner's statement of reasons for allowance: The closest prior art of record is Rhoads (US 5,636,292), Brundrett et al. (US 6,249,866), Orrin et al. (US

6,011,849), Coppersmith et al. (US 5,454,039), StegFS: “A Steganographic File System” PANG et al., "The Steganographic File System" Anderson et al., and “GBDE - GEOM Based Disk Encryption" Poul-Henning Kamp. While all of the prior art mentioned above deals with encryption of files or a file system, they do not individually or in combination disclose all of the limitations within the instant application. Specifically the claimed language of the instant application provides a conventional file index and files referenced by a file index which are separately, steganographically encrypted onto a storage device. While the prior art does provide files which are encrypted, a smaller subset provide steganographic encryption which is specifically used to hide the existence of data and no reference provides a file index which is encoded separately and using a different process than that of the data which is referenced. Originally the examiner made a rejection which combines a conventional file system with conventional steganographic encryption. The only manner in which obviousness can be maintained in this scenario is if a static file system including the index and all files is taken as an entire block and encrypted. Of course in this scenario, encryption would not be with separate processes, but with one unified process causing the data to be locked in the current image instead of the updatable manner described within the instant application. While the examiner feels that it may have been “obvious to try” encrypting via separate processes in order to allow easier ability to update, this is not show with any of the above referenced prior art and additionally overcoming the deficiencies provided with a simple combination are not in themselves obvious and require an inventive step.

The dependent claims which are definite and enable by the specification and being further limiting to the independent claims are also allowed.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled “Comments on Statement of Reasons for Allowance.”

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRUCE A. WITZENBURG whose telephone number is (571)270-1908. The examiner can normally be reached on M-F 9:00 - 6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner’s supervisor, Hosain Alam can be reached on 571-272-3978. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Bruce A Witzenburg/

Examiner, Art Unit 2166

/Etienne P LeRoux/

Primary Examiner, Art Unit 2161